PR4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/935,130	08/21/2001	Limor Schweitzer	XACTP014C	9607

28875 7590 05/18/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
NGUYEN, HAI V	
ART UNIT	**PAPER NUMBER**
2142	14

DATE MAILED: 05/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/935,130	SCHWEITZER ET AL.	
	Examiner	Art Unit	
	Hai V. Nguyen	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *32-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *32-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the communication received on 22 April 2004.

2. Claims 32-47 are presented for communication.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 32-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Herbert** U.S. patent no. **5,333,183** in view of **Gavan** et al. U.S. patent no. **6,601,048 B1**.

5. As to claim 32, Herbert, Universal MDR data Record Collection And Reporting System, discloses the invention as claimed, including a method for database management and recovery, comprising:

(a) collecting network communications usage information in real-time from a plurality of network devices utilizing a plurality of information source modules *(Herbert, Abstract, Figs. 5, 8, 20; cols. 22-23, table 4)*; However, Herbert does not explicitly disclose filtering and aggregating the network communications usage information utilizing a plurality of gatherers, *wherein the filtering and aggregating are based on a user-defined configuration*. Thus, the artisan would have been motivated to look into the related the network management art for potential methods and systems for implementing the filtering and aggregating the network communications usage

information utilizing a plurality of gatherers, *wherein the filtering and aggregating are based on a user-defined configuration.*

In the same field of endeavor, Gavan, related System And Method For Detecting and Managing Fraud, discloses in an analogous art distributed data network. Gavan discloses in the *Figs. 1 and 8 that the analysis layer to filter and to consolidate and correlate and to reduce alarms into cases. Correlation is governed by analysis rules which can be programmed and kept in a rules database. Rules are configurable and can use the probability of fraud which was assigned by profiling processor as a parameter. For example, a rule can state "only build cases from alarms having greater than 50% probability of fraud and which are generated for the same account (Gavan, Abstract; col. 2, lines 18-28; col. 3, line 67 – col. 4, line 37; col. 6, lines 35-51; col. 7, lines 28-35; col. 11, lines 54-65; col. 12, lines 6-37; col. 26, line 45 – col. 27, line 62).* Accordingly, it would have been obvious to one of ordinary skill in the networking computing art at the time the invention was made to have incorporated Gavan's teachings of user-defined configuration *(Gavan, Abstract; col. 6, line 65 – col. 7, line 45)* with the teachings of Herbert, *for the purpose of providing flexibility and permitting substantial tailoring of the system to user-specific situation (Gavan, col. 7, lines 1-45).*

Herbert-Gavan discloses (b) filtering and aggregating the network communications usage information utilizing a plurality of gatherers *(Herbert, col. 15, table 7(b); col. 21, table 3(b); Gavan, Fig. 1, item 123)*;

Herbert-Gavan discloses (c) completing a plurality of data records from the filtered and aggregated network communications usage information utilizing a central

event manager *(Gavan, Fig. 1, item 140)*, the plurality of data records corresponding to network usage by a plurality of users *(Herbert, cols. 24-25, table 5; Gavan, Fig. 1,item 139; col. 12, lines 30-37; col. 28, line 12 – col. 30, line 10);*

Herbert-Gavan discloses (d) storing the plurality of data records in a database *(Herbert, col. 6, lines 47-60; Gavan, Fig. 1, item 138; col. 12, lines 30-37)*;

Herbert-Gavan discloses (e) continuously monitoring a state of the gatherers *(Herbert, col. 13, line 2 – col. 14, line 50; Gavan, Abstract, col. 10, line 30 – col. 11, line 48)*;

Herbert-Gavan discloses (f) detecting a fault *(Herbert, col. 13, line 50 – col. 14, line 10; Gavan, col. 10, line 27 – col. 11, line 48)*; and

Herbert-Gavan discloses (g) utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof *(Herbert, cols. 25-26, table 5; Gavan, col. 30, lines 11-63).*

6. As to claim 33, Herbert-Gavan discloses, wherein the data records are stored in the database at a user-specific interval *(Herbert, col. 10, table 1, element A6; Gavan, Abstract, col. 7, line 35 – col. 8, line 19).*

7. As to claim 34, Herbert-Gavan discloses, further comprising time stamping the stored data records *(Herbert, cols. 25-26, table 5; Gavan, Abstract, col. 7, line 35 – col. 8, line 19).*

8. As to claim 35, Herbert-Gavan discloses, further comprising deleting the stored data records upon the cessation of a predetermined amount of time after the storage

utilizing the timestamp *(Herbert, cols. 23-24, table 5; Gavan, Abstract, col. 7, line 35 – col. 8, line 19)*.

9. As to claim 36, Herbert-Gavan discloses, further comprising caching the network communications usage information collected from the network devices utilizing the gatherers *(Herbert, Fig. 12, item 216; col. 29, line 49 – col. 30, line 25; Gavan, Abstract, col. 7, line 35 – col. 8, line 19; col. 10, line 40 col. 11, line 35)*.

10. Claim 37 is corresponding computer program product residing on computer readable medium claim of claim 32; therefore it is rejected under the same rationale as claim 32.

11. Claims 38-41 are substantially the same as claims 33-36 and thus they are rejected under the same rationale as claims 33-36.

12. Claim 42 is corresponding system claim of claim 32; therefore it is rejected under the same rationale as claim 32.

13. Claims 43-46 are substantially the same as claims 33-36 and thus they are rejected under the same rationale as claims 33-36.

14. As to claim 47, Herbert-Gavan discloses a method for database management and recovery, comprising:

(a) collecting network communications usage information in real-time from network devices at a plurality of layers utilizing multiple gatherers each including a plurality of information source modules each interfacing with one of the network devices and capable of communicating using a protocol specific to the network device coupled thereto, the network devices selected from the group consisting of routers, switches,

firewalls, authentication servers, web hosts, proxy servers, netflow servers, databases, mail servers, RADIUS servers, and domain name servers, the gatherers being positioned on a segment of the network on which the network devices coupled thereto are positioned for minimizing an impact of the gatherers on the network *(Herbert, Abstract, Figs. 5, 8, 20; Gavan, Fig. 1; col. 2, lines 17-44; col. 8, line 30 – col. 9, line 65)*;

(b) translating the network communications usage information collected from the network devices utilizing the information source modules *(Gavan, Fig. 1, items 123, 125, 128, 132)*;

(c) caching the network communications usage information collected from the network devices utilizing the gatherers *(Gavan, Fig. 1, items 119, 120)*;

(d) normalizing the network communications usage information with the gatherers by excluding fields not required by a central event manager coupled to the gatherers *(Gavan, Fig. 1, item 124; col. 10, line 26-60; col. 14, line 30 – col. 15, line 24)*;

(e) defining an enhancement procedure utilizing the central event manager *(Gavan, Fig. 4; Fig. 5A, item 510; col. 17, line 20 col. 18, line 60)*;

(f) coordinating the collection of the network communications usage information by the gatherers utilizing the central event manager *(Gavan, Fig. 1,item 139 or 140; col. 12, lines 30-37; col. 28, line 12 – col. 30, line 10)*;

(g) filtering the network communications usage information utilizing the central event manager *(Gavan, Fig. 1,item 139 or 140; col. 12, lines 30-37; col. 28, line 12 – col. 30, line 10)*;

(h) completing a plurality of data records from the filtered network communications usage information, the plurality of data records corresponding to network usage by a plurality of users *(Gavan, Fig. 1,item 139 or 140; col. 12, lines 30-37; col. 28, line 12 – col. 30, line 10)*;

(i) aggregating the network communications usage information and the data records utilizing the central event manager for reducing a number of the data records *(Gavan, Fig. 1,item 139 or 140; col. 12, lines 30-37; col. 27, line 44 – col. 28, line 10; col. 28, line 12 – col. 30, line 10)*;

(j) enhancing the aggregation of the network communications usage information with the gatherers in accordance with the defined enhancement procedure *(Gavan, Fig. 1,item 139 or 140; col. 11, line 35 - col. 12, lines 37; col. 28, line 12 – col. 30, line 10)*;

(k) time stamping the data records *(Gavan, col. 7, line 35 – col. 8, line 19)*;

(l) storing the time stamped data records in tables in a central database coupled to the central event manager at a user-specified interval *(Gavan, col. 17,line 4 – col. 18, line 60)*;

(m) deleting the stored data records upon the cessation of a predetermined amount of time after the storage utilizing the timestamp *(Gavan, col. 17,line 4 – col. 18, line 60)*;

(n) continuously monitoring a state of the gatherers *(Herbert, col. 13, line 2 – col. 14, line 50; Gavan, Abstract, col. 10, line 30 – col. 11, line 48)*;

(o) detecting a fault *(Herbert, col. 13, line 50 – col. 14, line 10; Gavan, col. 10, line 27 – col. 11, line 48)*; and

(p) utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof *(Herbert, cols. 25-26, table 5; Gavan, col. 30, lines 11-63)*.

15. Claim 47 is substantially similar limitations of claims 32-36 and therefore, it is rejected for the same reasons set for those in the rejection of claims 32-36.

16. Further references of interest are cited on Form PTO-892, which is an attachment to this action.

Conclusion

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hai V. Nguyen whose telephone number is 703-306-0276. The examiner can normally be reached on 6:00-3:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jack Harvey can be reached on 703-305-9705. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Hai V. Nguyen
Examiner
Art Unit 2142

JACK B. HARVEY
SUPERVISORY PATENT EXAMINER